

U.S. DISTRICT COURT
DISTRICT OF MARYLAND

2017 JUL 18 PM 4:57

ZAM: USAO#2015R000687

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

CLERK'S OFFICE
AT BALTIMORE
BY _____ DEPUTY

UNITED STATES OF AMERICA

v.

SHANNON L. STAFFORD,

Defendant

CRIMINAL NO. JFM-17-0380

(Intentional Damage to a Protected
Computer, 18 U.S.C. §§ 1030(a)(5)(A)
and (c)(4)(B); Attempted Intentional
Damage to a Protected Computer,
18 U.S.C. §§ 1030(a)(5)(A), (b) and
(c)(4)(B); Forfeiture, 18 U.S.C. §§ 1030(i)
and 982(a)(2)(B))

INDICTMENT

COUNT ONE

(Intentional Damage to a Protected Computer)

The Grand Jury for the District of Maryland charges that:

Introduction

At all times material to this Indictment:

The Defendant and the Victim Business

1. SHANNON L. STAFFORD was a resident of Crofton, Maryland.
2. "Business A" was a global company with thousands of employees, and offices around the world, including in Maryland. The computer systems of Business A were used in and affected interstate and foreign commerce.

STAFFORD's Employment with Business A

3. Beginning on or about January 5, 2004, and continuing until on or about August 6, 2015, STAFFORD worked in the information technology ("IT") department in the Washington, D.C., offices of Business A.
4. STAFFORD provided IT technical support and assistance for employees of

Business A in the Washington, D.C., and Baltimore, Maryland, offices of Business A. **STAFFORD** provided IT technical support and assistance to employees of Business A who were visiting Baltimore or Washington, D.C., from other locations.

5. As part of his regular duties at Business A, **STAFFORD** had access to the system login credentials of other employees. Business A authorized **STAFFORD** to use the system login credentials of other employees so that **STAFFORD** could provide the Business A employees with IT technical support and assistance.

6. As part of his regular duties at Business A, **STAFFORD** disabled the computer system access credentials at the end of a person's employment at Business A. **STAFFORD** was aware that former employees of Business A were no longer authorized to access Business A's computer systems.

7. On or about August 6, 2015, Business A terminated **STAFFORD**'s employment.

STAFFORD's Intentional Damage to the Computer Systems of Business A

8. Users who are not directly connected to Business A's internal network can access the network remotely via a virtual private network (VPN) connection.

9. On or about the evening of August 6, 2015, after **STAFFORD** attempted to access the computer systems of Business A remotely, through the business's VPN from his residence in Crofton, Maryland. **STAFFORD** unsuccessfully attempted to access the computer systems of Business A without authorization approximately 10 times, using his own user credentials and credentials that were not his, including the credentials of employees of Business A who he had previously assisted. **STAFFORD** was eventually able to successfully access the computer systems of Business A using the credentials of Person 1, an employee of Business A who he had previously assisted.

10. On or about August 8, 2015, **STAFFORD** used the credentials of Person 1 to access

the computer systems of Business A without authorization from his residence in Crofton, Maryland. During his unauthorized access, **STAFFORD** accessed a computer in the IT department of Business A's Washington, D.C. office.

11. **STAFFORD** used the Washington, DC, IT computer to execute commands to delete six Storage Area Network (SAN) file storage drives, causing severe disruption to Business A's operations. As a result of **STAFFORD**'s deletion of the network file storage drives, Business A's computer network was shut down for approximately 36 hours, until the deleted data could be restored from backups.

12. On or about August 10, 2015, Business A reset the network passwords of all employees in its Baltimore, Maryland, and Washington, D.C., offices.

13. On or about August 11, 2015, **STAFFORD** unsuccessfully attempted to access the computer systems of Business A without authorization approximately 13 times, using credentials that were not his, including the credentials of employees of Business A who he had previously assisted.

14. On or about August 13, 2015, representatives of Business A contacted **STAFFORD** and demanded that he cease and desist his unlawful access to the company's systems.

15. On or about August 21, 2015 and September 9, 2015, **STAFFORD** unsuccessfully attempted to access the computer systems of Business A without authorization approximately 17 times, using credentials that were not his, including the credentials of employees of Business A who he had previously assisted.

16. On or about September 14, 2015, **STAFFORD** used the credentials of Person 2 to access the computer systems of Business A without authorization from his residence in Crofton, Maryland. Person 2 was an employee of Business A who he had previously assisted. During his unauthorized access, **STAFFORD** attempted to access network file storage computer in the IT

department of Business A's Baltimore office.

The Charge

17. On or about August 8, 2015, in the District of Maryland and elsewhere, the defendant,

SHANNON L. STAFFORD,

knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct intentionally caused damage without authorization, to a protected computer, the computer systems of Business A, a company engaged in business and communications in interstate and foreign commerce, and **STAFFORD's** conduct caused losses to Business A aggregating at least \$5,000 in value.

18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)

COUNT TWO

(Attempted Intentional Damage to a Protected Computer)

The Grand Jury for the District of Maryland further charges that:

1. The allegations of Paragraphs 1 through 16 of Count One are incorporated here.
2. Between and including on or about August 8, 2015 and September 14, 2015, in the District of Maryland and elsewhere, the defendant,

SHANNON L. STAFFORD,

knowingly caused and attempted to cause the transmission of a program, information, code, and command, intending to cause damage, without authorization, to a protected computer, the computer systems of Business A, a company engaged in business and communications in interstate and foreign commerce, and **STAFFORD's** conduct would have caused losses to Business A aggregating at least \$5,000 in value.

18 U.S.C. §§ 1030(a)(5)(A), (b) and (c)(4)(B)

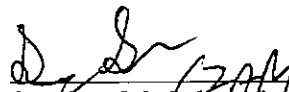
FORFEITURE

As a result of a conviction for either of the offenses set forth in this Indictment, the defendant,

SHANNON L. STAFFORD,

shall forfeit to the United States his interest in all property, real and personal, that was used, or intended to be used, to commit or to promote the commission of the offense, including but not limited to (1) an Apple MacBook Pro 13" with Retina display (Serial Number: C02N30DAFH05), seized from his residence on November 3, 2015; (2) a Silver Apple MacBook Pro Laptop Model A1260, (Serial Number: W88101TAYKO); and, (3) any property traceable to such property, or that constitutes or is traceable to gross profits or other proceeds obtained, directly or indirectly from the offense.

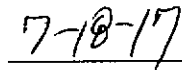
18 U.S.C. §§ 1030(i) and 982(a)(2)(B)


Stephen M. Schenning
Acting United States Attorney

A TRUE BILL:

SIGNATURE REDACTED

Foreperson


Date